Introduzione

di *Costantino Cipolla*[*] e *Annalisa Plava*[♦]

La rivoluzione digitale che – in poco meno di dieci anni –, si è insinuata nelle viscere sociali, economiche e politiche dei cittadini del mondo reale e digitale, ha inciso, in maniera determinante, su orientamenti, azioni, pensieri.

La *web society*, potenzialmente senza tempo e senza spazio (Castells, 2004, 2008), ci permette, attraverso o supportati da dispositivi, di muoverci con disinvoltura all'interno dei più diversificati angoli della Rete coinvolti (più o meno consapevolmente) dall'intermittenza delle luci e delle ombre di cui la digitalizzazione della società contemporanea è portatrice. È proprio questa discontinuità di illuminazione che interessa questo numero della rivista. Gettare bagliore sulle ombre di questo sfavillante mondo connesso per renderci un po' meno ingenui e un po' più consapevoli.

Computer, *smartphone* e *devices* indossabili incarnano i mezzi o sono la causa anche della digitalizzazione del crimine. A diversi livelli e coinvolgendo le più variegate forme dell'illegalità, l'evolversi del cosiddetto *internet of things* – una connessione capillare di qualsiasi strumento in rete ICT – permette una semplificazione nel possibile sfruttamento dei dati e delle informazioni degli utenti ed un aumento dei rischi nel subire azioni criminose commesse con o attraverso *software* digitali (Jori, 2013). La dimensione virtuale del reato prende l'accezione di *computer crime* o *computer related crime* a seconda che il crimine sia dovuto al risvolto negativo che lo sviluppo tecnologico ha determinato o che si tratti di crimini dove il computer (e i suoi annessi) rappresentano i mezzi attraverso cui si evolvono i crimini "tradizionali".

Non si tratta, dunque, di meri strumenti attraverso i quali possono essere commessi degli atti illeciti ma vere e proprie *crime scenes* in cui interviene,

[*] Università di Bologna - Dipartimento di Sociologia e Diritto dell'Economia.
costantino.cipolla@unibo.it

[♦] Università di Bologna - Dipartimento di Sociologia e Diritto dell'Economia.
annalisa.plava2@unibo.it

Sicurezza e scienze sociali V, 3/2017, ISSN 2283-8740, ISSNe 2283-7523
DOI: 10.3280/SISS2017-003002

Copyright © FrancoAngeli
N.B: Copia ad uso personale. È vietata la riproduzione (totale o parziale) dell'opera con qualsiasi mezzo effettuata e la sua messa a disposizione di terzi, sia in forma gratuita sia a pagamento.

in prima linea, la propria identità. E alla fine, tutto risulta fortemente sovraesposto e condiviso.

Cosa intendiamo, quindi, per sicurezza ma soprattutto per insicurezza, oggi? E la paura e il terrore diffusi da eventi tanto improvvisi quanto eclatanti, dichiarati in maniera agghiacciante attraverso la pervasività di ogni mezzo di comunicazione socio-digitale? Dove possiamo rifugiarci quando la voglia di scappare ci atterrisce e ci rende inermi e bloccati in un mondo tanto vasto quanto vulnerabile?

Federici e Sorrentino aprono la sezione saggi con considerazioni che cercano un'interpretazione innovativa alla sicurezza in Rete. Focalizzandosi sulla dimensione sociale del problema, da un lato fanno emergere gli utenti e il loro quotidiano scontro con il caotico impatto di una complessità difficile da individuare e da prevedere; dall'altro l'idea di *cybersecurity* rinforzata da un'educazione e una formazione all'uso consapevole di Internet diventano la condizione per proteggere lo spazio cibernetico davanti ad una criminalità *dark* e *clear*, sempre più specializzata ed esperta.

Se la *cybersecurity* apre la discussione saggistica sono le differenti forme e casistiche dei *cybercrimes* che poi si impadroniscono dei capitoli a seguire. A rilevare che per comprendere il crimine moderno "glocalizzato" (Bauman, 2014), non possiamo esimerci dall'analizzarlo anche dal punto di vista della dinamica *online*.

Anzitutto l'illusione di una forma anonima di navigazione e di espressione al fine di limitare le forme pervasive di sorveglianza in Rete, ben fortificata dall'armatura dello pseudonimo, del *desktop* o dell'algoritmo criptato, è solo uno dei tratti che potrebbe condurre a devianza e antisocialità. Se in Internet, appare molto semplice sostituire o costruire false identità, il *fil rouge* di Brighi ci conduce verso una profonda riflessione sull'anonimato comparato al rapporto con identità, tutela delle libertà personali e sicurezza informatica. Il ragionamento cerca un approdo conclusivo, poi, verso il tentativo di formulare un'effettiva azione di prevenzione del crimine in situazioni conflittuali.

Percezioni differenti definiscono le reazioni e le preoccupazioni dei potenziali bersagli oppure atti di coraggio ci portano ad adattarci a un mondo che sembra assumere le dimensioni di un campo minato sul quale, da un momento all'altro, può brillare una mina?

Un campo minato mutevole, in cui i giocatori devono usare l'astuzia e le abilità della mente per ripulire o scoprire i numeri senza rischiare un'esplosione.

Un campo minato sul quale imparare a muoversi segnando, di volta in volta, con una bandierina i quadrati sui quali non passare.

Copyright © FrancoAngeli
N.B: Copia ad uso personale. È vietata la riproduzione (totale o parziale) dell'opera con qualsiasi mezzo effettuata e la sua messa a disposizione di terzi, sia in forma gratuita sia a pagamento.

Ma il percorso non è sempre raggiungibile senza effettuare tentativi di fortuna, non esiste un metodo certo di andatura, ecco perché non vi si può giocare in maniera perfetta.

Si può tentare, però, di trovare la strategia migliore al fine di assicurarsi la risoluzione dello schema casuale con la minima probabilità di incorrere in un'esplosione (Aiolli, 2013).

Crimini accomunati dall'obiettivo di colpire con violenza, più o meno organizzata, le proprie vittime attraverso i dispositivi tecnologici vengono illustrati, secondo angolature differenti da Franco, Buoncompagni, Plava e Mariano Angioni. Gli autori, infatti, mettono in rilievo quella sezione dei reati informatici che utilizzano i dispositivi connessi per raggiungere e perseguitare una persona in modo oppressivo, osceno, minaccioso e violento.

Franco si occupa di analizzare il rapporto tra donna e *web*. Una relazione che se da un punto di vista legislativo evidenzia delle notevoli conquiste sembra rimanere, però, intrappolato dal substrato socio-culturale. Complici, poi, i social media, la categoria sembra spesso divenire oggetto di *cyber-stalking*, *cyber*-molestia e *cyber*-violenza sessuale.

Nuove forme di violenza ed atteggiamenti devianti, hanno avuto un forte impatto anche sugli adolescenti, principale bacino d'utenza sia in qualità di vittime che di carnefici dei nuovi fenomeni di criminalità. Dal tratto simile al *cyber-bullying*, Buoncompagni si occupa dell'emergente fenomeno delle *cyber-gangs*. Quest'ultime, utilizzano in modo sempre più strategico i *social networks*: costruiscono e rafforzano identità off e online, si autocelebrano attraverso la distribuzione di foto e video, affermano la loro capacità operativa attraverso percosse, torture ed omicidi. E sono ancora i *social networks* ad interessare anche l'analisi sulle *Social Challenges* di Plava. Le logiche di *gamification* (Whitson, 2013) che attirano la quotidianità simbolica e algoritmica dei nativi digitali verso "sfide" lanciate sul *web* possono rivelarsi tanto ludiche quanto pericolose.

Conclude l'analisi sull'uso di Internet con uno sguardo anche ai *social networks*, il contributo di Mariano Angioni. L'autore si occupa dell'eversione *online* a scopo terroristico. Fermo restando che il contemporaneo ed allarmante terrorismo di matrice islamica sembra, ad oggi, preferire ancora esprimersi con azioni più canoniche, il documento cerca di capire come la normativa italiana sul terrorismo possa applicarsi nel suo corrispettivo informatico.

Entrando nella sezione delle cosiddette Esperienze, Lorenzo Angioni propone una prima indagine sulle tecniche e le tecnologie criminalistiche che l'investigazione di polizia scientifica ha sviluppato e utilizza per la ricerca

Copyright © FrancoAngeli
N.B: Copia ad uso personale. È vietata la riproduzione (totale o parziale) dell'opera con qualsiasi mezzo effettuata e la sua messa a disposizione di terzi, sia in forma gratuita sia a pagamento.

del dato digitale. In un'ottica evolutiva e ai fini del repertamento investigativo, viene illustrata la *Digital Forensic* su supporti hardware e le tecniche di *Anti-forensic*, atte a contrastare l'investigazione digitale. Su questa stessa direzione, interessante poi è l'attenzione posta dalla prospettiva di Amoroso che apre le porte – da perito informatico – alla comparazione forense tra giudici e parti.

A rinforzo di questa tematica arrivano i *cold cases* analizzati da Bardari, Brighi e Cazzola. Attraverso una serie di esperienze sul campo che si riferiscono a casi rimasti insoluti, si mostrano i metodi e gli strumenti d'analisi dell'informatica forense uniti alle moderne tecnologie al fine del repertamento informatico su base probatoria.

L'apertura pratica e concreta verso la discussione sulla progettazione di politiche preventive della violenza online, poi, viene illustrata da Deriu. L'autrice, dopo una prima rassegna delle diverse forme di violenza esercitate attraverso la Rete, evidenzia in che modo i *big data* costituiscano un valido supporto all'attività investigativa e come la disponibilità di queste nuove fonti informative abbia contribuito a ridisegnare le strategie investigative tradizionali.

Uno sguardo mirato agli adolescenti e alla prevenzione educativa *online*, viene segnalato dai co-autori Orazi e Fornari anche nel complesso rapporto, talvolta distorsivo, con i mezzi di comunicazione.

Sul versante internazionale Dominici prende in considerazione le c.d. "post verità" e tutta la problematica che informazioni approssimate o una volontaria disinformazione lanciata in Rete possa determinare nei suoi imprevedibili risvolti su scala, appunto, globale. L'autore, ragionando sia secondo il canonico quadro teorico-pratico-applicativo d'emergenza sia considerando i "fattori sociali e culturali", cerca il metodo più efficace di adattamento, interazione e miglioramento della qualità delle moderne democrazie.

I due *focus* finali, infine, mettono l'accento sulla spinosa diatriba tra sicurezza e libertà in Rete.

La sicurezza nella sua declinazione garantista alla *privacy* viene attentamente analizzata da Perillo, il quale pone l'attenzione su uno dei nuovi strumenti normativi per la prevenzione alla criminalità *online*: il Regolamento Generale sulla Protezione dei Dati.

Mentre scopriamo, attraverso una serie di situazioni realmente accadute, quale sia il "prezzo" che, spesso inconsapevolmente, paghiamo in Rete. Una libertà con annesse insidie derivanti da un uso troppo disinvolto dei dispositivi informatici che ci viene illustrata dal contributo conclusivo di Zecchi e Bertaccini.

Copyright © FrancoAngeli
N.B: Copia ad uso personale. È vietata la riproduzione (totale o parziale) dell'opera con qualsiasi mezzo effettuata e la sua messa a disposizione di terzi, sia in forma gratuita sia a pagamento.

Il presente numero ambisce ad analizzare il crimine *online* nella sua accezione più vasta coinvolgendo un tempo in cui gli uomini vivono soprattutto connessi. Vivono di dati, informazioni e *gap* generazionali a confronto che si aggrovigliano attraverso strumenti diretti verso una cultura convergente (Jenkins, 2007). Un tempo in cui l'insieme delle tradizioni e dei comportamenti trasmessi e utilizzati dal consorzio sociale virtuale fanno convergere il contenuto delle proprie interazioni all'interno di più piattaforme e processi tecno-industriali modificando le modalità di espressione quotidiana, la multifunzionalità, l'interazione, la partecipazione, l'apprendimento. Un tempo in cui ciascun utente, abitante del mondo reale che si trasporta anche nel virtuale, sceglie di essere attore attivo e/o passivo dinanzi a fenomeni ed eventi che capitano in maniera, in parte diretta, sul suo percorso. Un tempo che ha messo a disposizione di chiunque tutta una serie di informazioni istituzionali e "sicuritarie" che forniscono tante possibilità quante detrazioni.

Internet incentiva un tipo di spazio aperto e degli strumenti che, democraticamente, sono forniti agli utenti senza distinzione di intenti. Questo processo di digitalizzazione, pertanto, ha normalizzato comportamenti, semplificato azioni e facilitato la commissione di crimini. Entrambi, dunque, sia afferenti al mondo della legalità che dell'illegalità, provano a controllare quello che è il nuovo crimine nel mondo *online*. E lo fanno non senza complicazioni di natura interpretativa, strutturale e giuridica, e non senza cercare una buona strategia che anticipi, miri e infine neutralizzi l'avversario.

Riferimenti bibliografici

Aiolli F. (2013). *Appunti di programmazione scientifica in Python*. Bologna: Esculapio.

Bauman Z. (2014). *La solitudine del cittadino globale*. Milano: Feltrinelli.

Castells M. (2004). *La città delle reti*. Padova: Marsilio.

Castells M. (2008). *La nascita della società in rete*. Milano: Università Bocconi.

Jenkins H. (2007). *Cultura Convergente*. Milano: Apogeo Edu.

Cipolla C. (2013). *Perché non possiamo non essere eclettici. Il sapere sociale nella web society*. Milano: FrancoAngeli.

Jori M.G. (2013). *Diritto, nuove tecnologie e comunicazione digitale*. Milano: Giuffrè.

Whitson J.R. (2013). Gaming the Quantified Self. *Surveillance & Society*, 11 (1/2): 163-176.

Copyright © FrancoAngeli
N.B: Copia ad uso personale. È vietata la riproduzione (totale o parziale) dell'opera con qualsiasi mezzo effettuata e la sua messa a disposizione di terzi, sia in forma gratuita sia a pagamento.